Een IT-auditverklarin 'van nationaal belang'

NOREA pleit voor invoering van een IT-auditverklaring, die assurance geeft bij een IT-verslag. Bestuurders en stakeholders reageren overwegend positief. Maar er klinkt ook kritiek, vooral vanuit cyberbeveiligers. Wat voegt een IT-auditverklaring toe?

TEKST **BJÖRN REMMERSWAAL** BEELD **SHUTTERSTOCK**

Op 12 augustus 2021 kopte het FD 'Nieuwe IT-check kan voorwaarde worden voor krediet aan bedrijf'. Strekking van het verhaal: investeerders en banken willen graag weten of een organisatie de IT-beheersing goed op orde heeft, voordat ze financiering verlenen.
De afgelopen jaren toonden duidelijk aan dat gebrekkige cybersecurity vergaande gevolgen kan hebben; een flink aantal bedrijven werd getroffen door zogenoemde *ransomware*-aanvallen, waarbij soms miljoenen euro's aan *hackers* moesten worden betaald om weer toegang te krijgen tot de IT-systemen. Dit soort aanvallen kunnen ontwrichtend werken voor het bedrijf zelf, maar ook voor de hele keten daarachter.

Startschot

In januari 2020 oppert Michiel Steltman, directeur van branche-organisatie Digitale Infrastructuur Nederland, in een interview met BNR dat het een goed idee zou zijn als er een soort assurance-verklaring komt voor IT-systemen. Hij pleit voor een "verplichte jaarlijkse IT-audit bij bedrijven en organisaties in de vitale infrastructuur van ons land", om zo vast te stellen of de IT en beveiliging op orde is. Daarbij maakt Steltman een vergelijking met de jaarlijkse accountantscontrole. Het is het startschot voor NOREA, de beroepsorganisatie van IT-auditors, om een werkgroep samen te stellen die dit idee moet gaan onderzoeken.
"Al bijna dertig jaar rust de verplichting op de accountant dat die in het kader van de controle van de jaarrekening een oordeel moet geven over de betrouwbaarheid van de gegevensverwerking", stelt Marc Welters, NOREA-bestuurslid/vice-voorzitter en partner bij EY. "In de praktijk doen zich twee knelpunten voor. Ten eerste is er een flinke diversiteit in hoe accountants omgaan met die verplichting. Ten tweede zit IT in de →

g is

haarvaten van bedrijfsprocessen en beoordeelt de IT-auditor enkel de IT in *scope* voor de jaarrekeningcontrole. Aan dat laatste moet de IT-auditverklaring iets doen."

NOREA geeft ook in een artikel op haar website aan dat de scope van een jaarrekeningcontrole momenteel te beperkt is om een adequaat oordeel te vellen over de inrichting van de IT-beheersorganisatie en de beheersing van IT. "Laat staan dat daarnaast ruimte is om bijvoorbeeld vast te stellen of een organisatie voldoende weerbaar is tegen cyberaanvallen en qua IT voorbereid is op de nabije toekomst."

Volgens de beroepsorganisatie kan de IT-auditverklaring dat gat vullen. Volgens Welters betekent dat in de praktijk dat er een verklaring moet komen die rekening houdt met alle verschillende type organisaties. "Qua IT-systemen is een bank een heel ander bedrijf dan bijvoorbeeld een zorginstelling. Risicoprofielen verschillen sterk tussen organisaties, dus elk type organisatie zal specifieke aspecten van de IT-systemen moeten beoordelen en daarover verslag moeten doen in een gestandaardiseerde vorm. Het management geeft daarbij vervolgens een verklaring af en de IT-auditor controleert aan het einde van de keten of dat klopt." Daarnaast moet de IT-verklaring ook iets zeggen over de toekomstbestendigheid van IT binnen organisaties, omdat dit volgens NOREA voor de verschillende stakeholders "het meest relevant" is.

Welters legt uit dat de werkgroep inmiddels anderhalf jaar bezig is om te onderzoeken waar de behoefte ligt en wat de marsroutes kunnen zijn. De beroepsorganisatie doet momenteel via een enquête ook onderzoek naar de specifieke informatiebehoefte van bestuurders en commissarissen op het gebied van IT-systemen en de behoefte voor een IT-auditverklaring lijkt er volgens Welters zeker te zijn. NOREA laat zich qua vorm inspireren door de nieuwe Corporate Sustainability Reporting Directive, de Europese richtlijn op het gebied van duurzaamheidsrapportage. "De verklaring die we momenteel voor ogen hebben is daarop gebaseerd."

Het beeld dat het om accountants gaat die een aantal dagen bijscholing hebben gedaan, is echt niet meer zo.

Belang

De beroepsorganisatie stelt dat een brede groep van stakeholders belang hecht aan zekerheid over de juiste werking van informatietechnologie. Volgens NOREA is rapporteren over de IT "van nationaal belang", want Nederland behoort tot een van de meest gedigitaliseerde landen ter wereld, met een vooraanstaande positie van Amsterdam als IT-hub.

In het FD spreekt Eumedion-directeur Rients Abma de hoop uit dat het IT-verslag vast onderdeel wordt van de controleverklaring. "Ik vind dat de accountant het nu al moet vermelden als een bedrijf waarop toezicht wordt gehouden, de IT niet op orde heeft." Een woordvoerder van zakenbank NIBC sluit niet uit dat de IT-auditverklaring "in de toekomst een voorwaarde wordt bij kredieten aan bedrijven die afhankelijk zijn van IT".

NOREA-voorzitter Irene Vettewinkel-Raymakers, tevens auditdirecteur bij ABN Amro, zegt tegenover de krant dat de IT-verklaring "belangrijk wordt voor commissarissen en investeerders". Ook BDO-partner Wido Dalhuisen benadrukt dat financiers graag zekerheid willen over IT-systemen, als ze met een bedrijf in zee gaan. Ondernemersorganisaties VNO-NCW en MKB Nederland willen eerst weten of de kosten voor een IT-verklaring voor kleinere bedrijven "behapbaar zijn" en hoe het zit met geheimhouding.

Kritiek

Maar er worden ook kanttekeningen gemaakt. IT-beveiligingsbedrijven en cybersecurity-experts laten zich in het FD kritisch uit over de plannen en zijn van mening dat de IT-auditverklaring weinig zal toevoegen. Daarnaast twijfelen ze of de expertise van de IT-auditors wel op het juiste niveau is. "Een echte techneut die de techniek snapt, staat over het algemeen niet te trappelen om bij een accountantskantoor te gaan werken", zegt Alex Bik, technisch directeur van BIT datacenters, tegen het FD. Enkele cybersecurityadviseurs denken dat de verklaring een "papieren, statische werkelijkheid" zal weergeven, terwijl de risico's waar het om draait voortdurend wisselen. Een ander kritiekpunt is dat het vooral bureaucratie oplevert en slechts een nieuwe manier van accountantskantoren is om geld te verdienen. Daarnaast wijst Bik nog op de bestaande ISO-certificeringen, die volgens hem al toezien op een betrouwbare verwerking van (persoons)gegevens en prima functioneren.

Gestandaardiseerde verklaringen voor alle sectoren zorgen voor meer zekerheid bij alle stakeholders.

NOREA

Nederland is het enige land ter wereld met een postmaster IT-auditopleiding. Wie na het eindexamen drie jaar relevante werkervaring heeft, kan zich als RE (Register EDP-auditor) inschrijven in het register van de Nederlandse Orde van Register EDP-auditors (NOREA). Momenteel telt dat register ongeveer 1.800 RE's. NOREA is geaccrediteerd door de NBA en houdt zicht op de kwaliteit van de beroepsuitoefening door RE's. Meer info is beschikbaar via norea.nl.

NOREA is het daarmee niet eens, aldus voorzitter Irene Vettewinkel-Raymakers. "Bij de ISO-certificering wordt niet gekeken naar wat er daadwerkelijk gebeurt bij een organisatie. Wij stellen ook vast of de maatregelen gedurende een langere periode werken. Dat gaat dus verder."
Wat betreft de kritiek over de deskundigheid geeft Welters aan dat er al een tijd lang een *shift* gaande is in de IT-auditwereld. "Vroeger waren IT-auditors vrijwel allemaal accountants die waren omgeschoold richting IT. Twee decennia geleden was veertig procent ook RA. Daarna is er een aanzienlijke instroom ontstaan vanuit de technische universiteiten, bijvoorbeeld vanuit de opleidingen informatica. Tegenwoordig is het aantal accountants minder dan een kwart. Driekwart is echt een 'enkelvoudige' IT-auditor en de helft daarvan heeft een technische achtergrond. Dus het beeld dat het om accountants gaat die een aantal dagen bijscholing hebben gedaan, is echt niet meer zo. Daarnaast zijn we continu in gesprek met universiteiten, waardoor IT-auditors zich tegenwoordig tijdens de opleiding al kunnen specialiseren in expertisegebieden zoals *data science*, *privacy* en *cybersecurity*."

Verdienmodel

Wat betreft het verdienmodel, is Welters eerlijk: "Natuurlijk, dit kan business genereren, maar dat is niet de primaire insteek. We hebben in de afgelopen jaren allerlei producten ontwikkeld die organisaties kunnen helpen op het gebied van cybersecurity en privacy en deze verklaring sluit daar goed op aan." Hij wijst daarnaast nogmaals op het belang van een adequate IT-beheersing van organisaties om onze concurrentiepositie als land te behouden. "De IT-auditverklaring zorgt er ook voor dat de wet beter wordt uitgevoerd. Gestandaardiseerde verklaringen voor alle sectoren zorgen voor meer zekerheid bij alle stakeholders."
Welters maakt zich geen illusies dat de IT-auditverklaring ervoor zal zorgen dat bedrijven niet meer worden gehackt, maar de kans wordt wel kleiner. "Wij zeggen weleens dat er twee soorten organisaties zijn: organisaties die al een keer zijn gehackt en organisaties die nog niet weten dat ze zijn gehackt. De kans is groot dat je als organisatie een keer aan de beurt bent. Met een IT-auditverklaring worden bedrijven gedwongen hun weerbaarheid naar een goed niveau te brengen, wat de schade in zo'n geval aanzienlijk kan beperken." ←